Cisco CCNA III

Chapitre 2 - Concepts et configuration de base d'un commutateur

Abdelali SAIDI

abdelali.saidi@gmail.com

Plan

Présentation du chapitre

Objectifs du chapitre

Dans ce chapitre, vous allez apprendre à effectuer les tâches suivantes :

- Résumer le fonctionnement d'Ethernet tel qu'il est défini pour les réseaux locaux de 100/1000 Mbits/s dans la norme IEEE 802.3
- Expliquer les fonctions permettant à un commutateur de transmettre des trames Ethernet sur un réseau local
- Configurer un commutateur en vue de son utilisation sur un réseau conçu pour des transmissions de la voix, de la vidéo et des données
- Configurer une sécurité de base sur un commutateur destiné à fonctionner sur un réseau conçu pour des transmissions de la voix, de la vidéo et des données

Plan

Principaux éléments des réseaux Ethernet

Détection de porteuse avec accès multiple (CSMA/CD)

L'ensemble de règles auquel Ethernet a recours est fondé sur la technologie détection de porteuse avec accès multiple (CSMA/CD) de la norme IEEE.

- Ecoute de porteuse : l'émetteur vérifie l'état d'utilisation du Média.
  - si un signal est détecté, l'émetteur patiente un moment
  - sinon, l'émetteur transmet son message
- Accès multiple : lorsque la distance entre les périphériques est importante par rapport à la latence du réseau, il se peut qu'un deuxième émetteur ne détecte pas l'utilisation du réseau et commence à transmettre également son message. Chose qui implique une collision
- Détection des collisions : chaque périphérique qui détecte une collision continue d'émettre jusqu'à ce que tous les périphériques du même réseau puissent la détecter

Principaux éléments des réseaux Ethernet

Communications Ethernet

Les communications dans un réseau local commuté surviennent sous trois formes :

- Monodiffusion : communication dans laquelle une trame est transmise depuis un hôte vers une destination spécifique
- Diffusion : communication dans laquelle une trame est transmise d'une adresse vers toutes les autres adresses existantes
- Multidiffusion : communication dans laquelle une trame est transmise à un groupe spécifique de périphériques ou de clients

Principaux éléments des réseaux Ethernet

Trame Ethernet

La structure de trame Ethernet ajoute des en-têtes et des queues de bande autour de l'unité de données de protocole (PDU) de la couche 3 afin d'encapsuler le message transmis :

IEEE 802.3

7	1	6	6	2	De 46 à 1500	4
Préambule	Délimiteur de début de trame	Adresse de destination	Adresse source	Longueur/ Type	En-tête et données 802.2	Séquence de contrôle de trame

Figure: Entête d'une Trame Ethernet

Principaux éléments des réseaux Ethernet

Trame Ethernet

- Préambule et délimiteur : ces huit premiers octets de la trame demandent essentiellement aux récepteurs de se préparer à recevoir une nouvelle trame
- Adresse MAC de destination : permet un périphérique de déterminer si une trame lui est adressée
- Adresse MAC source : identifie la carte réseau ou l'interface d'origine de la trame
- Longueur/Type : détermine quel protocole de couche supérieure est présent
- Séquence de contrôle de trame : permet de détecter les erreurs survenues dans une trame

Principaux éléments des réseaux Ethernet

Adresses MAC

Une adresse MAC Ethernet est une valeur binaire de 48 bits exprimée sur 12 chiffres hexadécimaux. Elle se compose de :

- l'identifiant unique d'organisation (24 bits) : Cette partie identifie le fabricant de la carte réseau. Elle se compose de trois champs :
  - Bit de diffusion ou multidiffusion (1 bit)
  - Bit d'adresse administrée localement (1 bit)
  - Numéro d'identifiant d'organisation (22 bits)
- numéro d'affectation du constructeur (24 bits): Partie de l'adresse MAC qui concerne le constructeur. Elle identifie de manière unique le matériel Ethernet.

Principaux éléments des réseaux Ethernet

Paramètres bidirectionnels

Deux types de paramètres bidirectionnels sont employés pour les communications dans un réseau Ethernet :

- Bidirectionnel non simultané :
  - Flux de données unidirectionnel
  - Risque de collision plus élevé
  - Connectivité avec le concentrateur
- Bidirectionnel simultané :
  - Communication point à point uniquement
  - Connexion au port commuté dédié
  - Aucun risque de collision
  - Circuit de détection de collision désactivé

Principaux éléments des réseaux Ethernet

Paramètres de port de commutateur

Le type du support utilisé implique la configuration des paramètres bidirectionnels du port. Les commutateurs Cisco Catalyst présentent trois paramètres :

- auto : définit l'auto-négociation pour le mode bidirectionnel
- full : définit le mode bidirectionnel simultané
- half : définit le mode bidirectionnel non simultané
- auto-MDIX : détecte le type de câble requis pour les connexions Ethernet cuivre, puis configure les interfaces en conséquence

Principaux éléments des réseaux Ethernet

Table d'adresses MAC du commutateur

L'enregistrement des adresses MAC et des ports associés dans la table de commutation suit le processus suivant:

1. Le commutateur reçoit une trame du PC_1 sur le port_1 en destination d'un PC_2
2. Le commutateur enregistre l'adresse MAC de PC_1 et port_1 sur table de routage (si ce n'est déjà fait)
3. Le commutateur diffuse la trame si PC_2 ne se trouve pas sur la table de commutation
4. Le commutateur enregistre l'adresse MAC de PC_2 et le port_2 lorsque PC_2 réponde
5. Si une nouvelle trame est destiné vers PC_2, le commutateur saura le port à utiliser depuis la table de commutation

Considération liées à la conception des réseaux Ethernet

- Bande passante et débit
- Domaines de collision
- Domaines de diffusion
- Latence du réseau
- Encombrement du réseau
- Segmentation des réseaux locaux
- Ponts et commutateurs
- Routeurs

Considération liées à la conception des réseaux locaux

Contrôle de la latence du réseau

- Tenir compte de la latence que génère chaque périphérique réseau
- L'utilisation inutile de périphérique de couche OSI supérieur

Considération liées à la conception des réseaux locaux

Suppression des goulots d'étranglement

Les goulots d'étranglement dans un réseau sont des emplacements où un encombrement trop élevé peut ralentir les performances du réseau

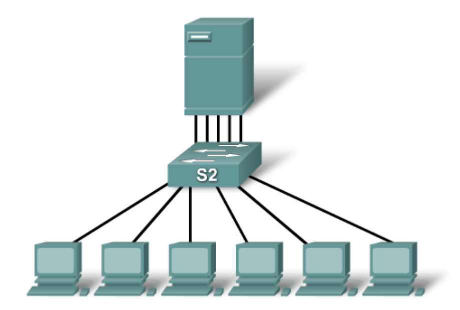


Figure: Suppression d'un goulot d'étranglement

Considération liées à la conception des réseaux locaux

Exercice 2.1.3.2

Plan

Méthodes de transmission par commutateur

Auparavant, les commutateurs faisaient appel aux méthodes de transmission pour la commutation des données entre des ports réseau :

- store and forward :
  - stockage en entier de la trame
  - contrôle d'erreur à l'aide du CRC
  - transfert de la trame si le CRC correspond
  - primordiale dans les réseaux convergents
- cut-through :
  - transmission de la trame dès la lecture de l'adresse MAC
  - aucun contrôle
  - plus rapide que "store and forward"
  - peut transmettre des trames endommagées

Commutation symétrique et asymétrique

Commutation symétrique et asymétrique

La commutation symétrique ou asymétrique d'un réseau local dépend de la façon dont la bande passante est allouée aux ports de commutateur

- Commutation symétrique : des connexions commutées entre des ports associés à des bandes passantes différentes
- Commutation asymétrique : tous les ports disposent de la même bande passante

Mise en mémoire tampon

Mise en mémoire tampon axée sur les ports et partagée

Il existe deux méthodes de mise en mémoire tampon :

- Mise en mémoire tampon axée sur les ports : les trames sont stockées dans des files d'attente liées à des ports entrants spécifiques;
- Mise en mémoire tampon partagée : stocke toutes les trames dans une mémoire tampon commune à tous les ports du commutateur.

Commutation sur les couches 2 et 3

Commutateur de couche 2

- permet d'effectuer une commutation et un filtrage en se basant uniquement sur l'adresse MAC
- est entièrement transparent pour les protocoles réseau et les applications utilisateur

Commutateur de couche 3

- fonctionne de manière similaire à un commutateur de couche 2
- peut également exploiter celles des adresses IP (routage de base)
- pour les connexions WAN il est préférable d'utiliser des routeurs dédiés

Commutation sur les couches 2 et 3

Exercices 2.2.4.3

Plan

Utilisation de l'ILC

Modes d'interface de ligne de commande

- Mode d'exécution utilisateur : permet d'accéder uniquement à un nombre de commandes de contrôle de base
- Mode d'exécution privilégié : permet d'accéder à toutes les commandes de configuration et de gestion.
- Mode de configuration globale : configurer les paramètres généraux
- Mode de configuration d'interface : configurer les paramètres d'une interface réseau

Utilisation de l'ILC

Commandes

- enable : Passez du mode d'exécution utilisateur au mode d'exécution privilégié
- disable : Passez du mode d'exécution privilégié au mode d'exécution utilisateur
- interface fastethernet 0/1 : Passez du mode de configuration globale au mode de configuration d'interface pour l'interface Fast Ethernet 0/1
- exit : passer d'un mode actuel au mode précédant

Utilisation de l'ILC

La fonction d'aide

L'ILC de Cisco IOS propose deux types d'aide :

- Aide sur les termes
- Aide relative à la syntaxe des commandes

Messages d'erreurs

Exemple de message d'erreur	Signification
`switch#`**`cl`** `% Ambiguous command: "cl"`	Vous n'avez pas entré suffisamment de caractères pour permettre à votre périphérique de reconnaître la commande.
`switch#`**`clock`** `% Incomplete command.`	Vous n'avez pas entré tous les mots clés ou les valeurs nécessaires pour cette commande.

`switch#`**`clock set aa:12:23`**
`^`
`% Invalid input detected at '^' marker.`
	Vous avez mal entré la commande. L'accent circonflexe (^) marque la position de l'erreur.

Utilisation de l'ILC

Mémoire tampon d'historique des commandes

La fonction d'historique des commandes vous permet d'accomplir les tâches suivantes :

- afficher le contenu de la mémoire tampon des commandes
- définir la taille de la mémoire tampon de l'historique des commandes

Commandes

- show history : affiche l'historique (par default les 10 dernières commandes)
- terminal history size 50 : configure la taille du tampon (entre 0 et 256 lignes)
- terminal no history size : rétablit la configuration par default
- terminal no history : désactive l'historique

Séquence d'amorçage d'un commutateur

Séquence d'amorçage d'un commutateur

- exécute le chargeur d'amorçage (stocké dans la NVRAM)
- Le chargeur d'amorçage effectue les opérations suivantes :
  - Il procède à une initialisation de l'unité centrale à un faible niveau
  - Il procède à un POST
  - Il initialise le système de fichiers flash sur la carte système
  - Il importe une image du système d'exploitation par défaut dans la mémoire et amorce le commutateur
- Le système d'exploitation initialise ensuite les interfaces à l'aide des commandes Cisco IOS disponibles dans le fichier de configuration du système d'exploitation (config.text) stocké dans la mémoire flash du commutateur.

Configuration de base d'un routeur

Gestion du commutateur à distance

- Attribution d'une adresse IP au commutateur
  - L'adresse IP est attribuée à une interface virtuelle
  - Il faut s'assurer que plusieurs ports du commutateur appartiennent au VLAN de gestion
  - Par default, VLAN1 est l'interface virtuelle de gestion
  - Il est recommandé d'utiliser VLAN 99
- Configuration de l'interface de gestion
  - travailler en mode de configuration d'interface de réseau local virtuel
  - affecter une adresse IP
  - activer l'interface

Configuration de base d'un routeur

Configuration de la passerelle par default

- Configurer la passerelle par default
- Vérification de la configuration
- Commande mdix auto : permet de détecter le type de câble requis pour les connexions Ethernet cuivre, puis configure les interfaces en conséquence

Configuration du mode bidirectionnel et de la vitesse d'un port

- duplex auto : Configurer le mode birectionnel d'interface pour activer la configuration bidirectionnelle automatique
- speed auto : Configurer la vitesse bidirectionnelle d'interface et activer la configuration de vitesse automatique

Configuration de base d'un routeur

Configuration d'une interface Web

- ip http authentication enable|local|tacacs : Configurer l'interface du serveur HTTP pour le type d'authentification
- ip http server : Activer le serveur HTTP

Configuration de base d'un routeur

Gestion de la table d'adresses MAC

Les commutateurs utilisent des tables d'adresses MAC pour déterminer le mode de transmission du trafic d'un port à l'autre. Ces tables MAC comprennent des adresses dynamiques et statiques.

- how mac-address-table : affiche la table de commutation
- Les adresses dynamiques sont des adresses MAC source que le commutateur assimile, puis définit comme obsolètes dès qu'elles ne sont plus utilisées (300 secondes)
- Les adresses statiques sont affecté par un administrateur réseau et ne sont jamais obsolètes
- (no) mac-address-table static ¡adresse_MAC¿ vlan 1-4096, ALL interface id_interface : active (désactive un mappage statique)

Configuration de base d'un routeur

Vérification de la configuration d'un commutateur

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Affiche l'état et la configuration d'une ou de l'ensemble des interfaces disponibles sur le commutateur.	`show interfaces [interface-id]`
Affiche le contenu de la configuration de démarrage.	`show startup-config`
Affiche la configuration actuelle.	`show running-config`
Affiche des informations sur le système de fichiers flash.	`show flash:`
Affiche l'état du logiciel et du matériel système.	`show version`
Affiche l'historique des commandes de session.	`show history`
Affiche des informations IP. L'option d'interface dévoile l'état et la configuration de l'interface IP. L'option http affiche les données HTTP relatives au gestionnaire de périphériques exécuté sur le commutateur. L'option arp affiche la table ARP IP.	`show ip {interface | http | arp}`
Affiche la la table de transmission MAC.	`show mac-address-table`

Configuration de base d'un routeur

Sauvegarde de la configuration

- copy system:running-config flash:startup-config
- copy running-config startup-config
- copy startup-config flash:config.bak1

Restauration de la configuration

- copy flash:config.bak1 startup-config
- reload

Configuration de base d'un routeur

Serveur tftp

Le stockage sécurisé de la configuration, loin du commutateur, permet de la protéger en cas de problème majeur et important avec votre commutateur.

- copy system:running-config tftp://adresse_IP/nom_fichier : sauvegarde la configuration sur un serveur tftp
- copy tftp://adresse_IP/nom_fichier system:running-config ou copy tftp://adresse_IP/nom_fichier nvram:startup-config : récupère une configuration depuis un serveur tftp

- Suppression des paramètres de configuration : erase nvram: ou erase startup-config en mode d'exécution privilégié.
- Suppression d'un fichier de configuration stocké : delete flash:nom_fichier en mode d'exécution privilégié

Plan

Configuration des options de mots de passe

Sécurisation de la console

- configure terminal
- line console
- password mdp
- login

Protection des ports vty

- configure terminal
- line vty 0 4
- password mdp
- login

Configuration des options de mots de passe

Configuration du mot de passe en mode d'exécution

- configure terminal
- enable password
- enable secret mdp

Remarque

Il est universellement reconnu que les mots de passe doivent être chiffrés et non stockés dans un format de texte clair. La commande Cisco IOS *service password-encryption* autorise le chiffrement des mots de passe de service.

Configuration des options de mots de passe

Récupération de mot de passe

Réellement, ce n'est pas une récupération de mot de passe, c'est une ré-initialisation. Les étapes sont:

1. Connexion physique au commutateur
2. Maintenez le bouton Mode enfoncé jusqu'à ce que le LED système devienne brièvement orange, puis prenne une couleur verte définitive
3. Initialisez le système de fichiers flash à l'aide de la commande flash_init
4. Chargez tous les fichiers d'aide au moyen de la commande load_helper

Configuration des options de mots de passe

Récupération de mot de passe

1. Affichez le contenu de la mémoire flash à l'aide de la commande dir flash :
2. Rename flash:config.text flash:config.text.old
3. Démarrez le système avec la commande boot
4. Empêcher le système de démarrer le programme de configuration
5. rename flash:config.text.old flash:config.text
6. copy flash:config.text system:running-config
7. enable secret mot de passe

Configuration des options de mots de passe

Bannière de connexion

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	Comm1#**configure terminal**
Configurer une bannière de connexion.	Comm1(config)#**banner login "Personnel autorisé uniquement"**

Bannière d'une MOTD

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	Comm1#**configure terminal**
Configurer une bannière MOTD.	Comm1(config)#**banner motd "La maintenance du périphérique aura lieu vendredi."**

Configuration des options de mots de passe

Telnet

- La méthode d'accès la plus courante
- Envoie de messages en clair
- Méthode non sécurisée
- Configuration :
  - line vty 0 15
  - transport input telnet

Configuration des options de mots de passe

SSH

- Envoie de messages chiffrés
- Méthode sécurisée
- Configuration :
  - ip domain-name mondomaine.com
  - crypto key generate rsa
  - ip ssh version 2
  - line vty 0 15
  - transport input SSH

Menaces fréquentes en terme de sécurité

Menaces

- Inondation d'adresses MAC : exploite la limitation au niveau de la mémoire du commutateur enregistrant la table des adresses MAC
  - Conséquence : un commutateur inondé passe en mode *fail-openagit* et agit tel un concentrateur
- Attaques par mystification : exemples: DHCP spoofing, DHCP flooding
  - Pour empêcher toute attaque DHCP, faites appel aux fonctions de sécurité des ports et de surveillance DHCP disponibles sur les commutateurs
- CDP (Cisco Discovery Protocol) : permet d'identifier les périphériques cisco voisins. Il transporte les infos relatifs aux périphériques de manière non sécurisée et n'utilise aucun système d'authentification. Il est préférable de le désactiver.

Configuration de la sécurité des ports

Objectifs de la sécurité des ports

- préciser un groupe d'adresses MAC sur un port;
- autoriser une seule adresse MAC sur un port;
- préciser que le port s'arrête automatiquement si des adresses MAC non autorisées sont détectées

Configuration de la sécurité des ports

Types d'adresses MAC sécurisées

Il existe plusieurs façons de configurer la sécurité des ports:

- Adresses MAC sécurisées statiques : les adresses MAC sont configurées manuellement à l'aide de la commande de configuration d'interface *switchport port-security mac-address adresse_mac*
- Adresses MAC sécurisées dynamiques : les adresses MAC sont assimilées de manière dynamique et stockées uniquement dans la table d'adresses
- Adresses MAC sécurisées rémanentes : vous pouvez configurer un port pour assimiler dynamiquement des adresses MAC, puis enregistrer ces dernières dans la configuration en cours

Configuration de la sécurité des ports

Modes de violation de sécurité

Il y a violation de la sécurité lorsque l'une des situations suivantes se présente :

- Le nombre maximal d'adresses MAC sécurisées a été ajouté dans la table d'adresses et une station dont l'adresse MAC ne figure pas dans cette table tente d'accéder à l'interface
- Une adresse assimilée ou configurée dans une interface sécurisée est visible sur une autre interface sécurisée dans le même réseau local virtuel

Les modes sont :

Mode de violation	Acheminement du trafic	Envoi d'un message syslog	Affichage d'un message d'erreur	Incrémentation du compteur de violation	Arrêt du port
Protect	Non	Non	Non	Non	Non
Restrict	Non	Oui	Non	Oui	Non
Shutdown	Non	Oui	Non	Oui	Oui

Configuration de la sécurité des ports

Vérification de la sécurité des ports

- show port-security [interface id_interface] : afficher les paramètres de sécurité des ports du commutateur ou de l'interface spécifiée
- show port-security [interface id_interface] : afficher toutes les adresses MAC sécurisées configurées

Configuration de la sécurité des ports

Sécurisation des ports inutilisés

Une méthode simple à laquelle nombre d'administrateurs ont recours pour mieux protéger leur réseau contre tout accès non autorisé est de désactiver tous les ports qui ne sont pas exploités sur un commutateur réseau.